Моделювання кібер інцидентів в мультиагентному середовищі NetLogo

https://doi.org/10.31713/MCIT.2024.060

Новосьолов Дмитро
Поліський національний університет
Житомир, Україна
Diman7842@gmail.com

Анотація **– В роботі розглянуто можливості мультиагентного середовища NetLogo для розв'язання задач імітаційного моделювання процесів забезпечення кібербезпеки, а також для аналізу моделей (підходів) реагування на інциденти в кіберпросторі. За основу обрано сімейство моделей SI(E)R поширення вірусу.**

Ключові слова – NetLogo, мультиагентне моделювання, поширення вірусу в мережі, SIR.

Вступ. Стійкість системи в контексті забезпечення кібербезпеки полягає в здатності системи:

-визначати вразливості;

-оцінювати ризики;

-адекватно реагувати на виклики та інциденти;

-відновлювати функціонування в мінімальні строки з залученням мінімальної кількості ресурсів.

Основна проблема полягає в неповноті апрорної інформації щодо вразливостей, загроз та ризиків. Тому застосування імітаційного моделювання дозволяє аналізувати різні сценарії і тим самим збільшувати інформаційну обізнаність щодо можливих наслідків кібер інцидентів, а отже надає можливість розробляти адекватні плани реагування та відновлення.

Основна частина. За основу даної наукової роботи було обрано модель “Virus on network”. Дана модель підходить для розгляду та дослідження так , як вона має найбільш приближені умови для розвитку вірусів в будь якій захищеній системі.

Для цього спочатку буде описано саму модель для її розуміння в майбутньому для того щоб наступні дії були зрозумілі.

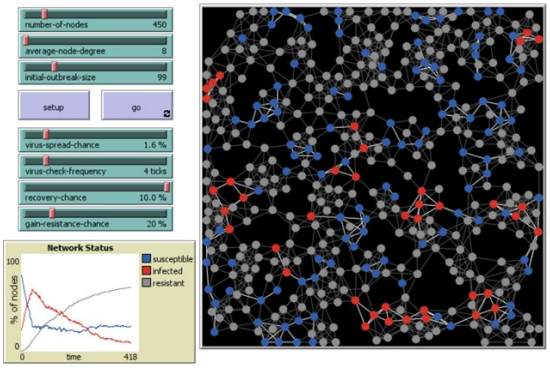

Рисунок 1 - модель Virus on network

Модель “Virus on Network” що зображена на Рисунку 1 використовується для симуляції поширення вірусу в мережі комп’ютерних вузлів, аналогічно до поширення комп’ютерних вірусів у кіберпросторі.

number-of-nodes (Кількість вузлів): Параметр, що визначає кількість комп'ютерів (вузлів) у мережі. Збільшення кількості вузлів розширює мережу, збільшуючи можливості для поширення вірусу.

average-node-degree (Середній ступінь вузла): Визначає середню кількість з'єднань (сусідів) у кожного вузла. Це параметр для моделювання рівня зв'язаності комп'ютерів і швидкості передачі вірусу.

initial-outbreak-size (Початковий розмір спалаху): Вказує кількість вузлів, заражених на початку моделювання. Збільшення цього параметра призводить до більшого початкового спалаху вірусу.

virus-spread-chance (Ймовірність поширення вірусу): Параметр, що визначає ймовірність поширення вірусу від зараженого вузла до сусіднього не зараженого. Вищі значення збільшують шанси на інфікування сусідів.

virus-check-frequency (Частота перевірки на вірус): Частота перевірки кожного вузла на наявність вірусу. Визначає, як часто вузли перевіряються на інфекцію або потребу в оновленні статусу.

recovery-chance (Ймовірність одужання): Визначає ймовірність того, що заражений вузол відновиться від вірусу і повернеться до нормального стану. Вищі значення сприяють швидкому зменшенню поширення вірусу.

gain-resistance-check (Частота перевірки на отримання стійкості): Частота перевірки вузла на можливість отримання стійкості до вірусу після одужання. Це дозволяє моделювати здатність вузла до отримання імунітету від подальшого зараження.

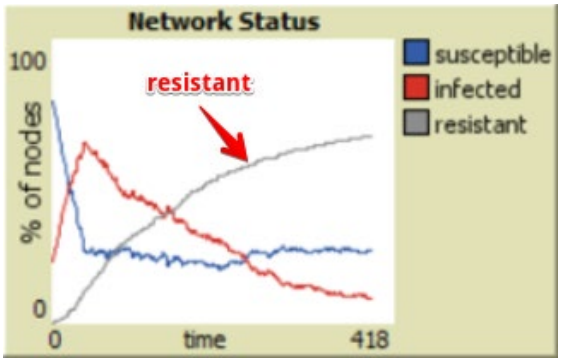

Рисунок 2 - відновлення системи

В даній роботі розглянемо virus-check-frequency , та її зміни з 1 пункту до 5, це значить , що система буде перевірятись частіше і шанс виявлення вірусів завчасно буде збільшено. Функція resistant показана на Рисунку 2 і в наступних Рисунках буде розглянуто саме її.

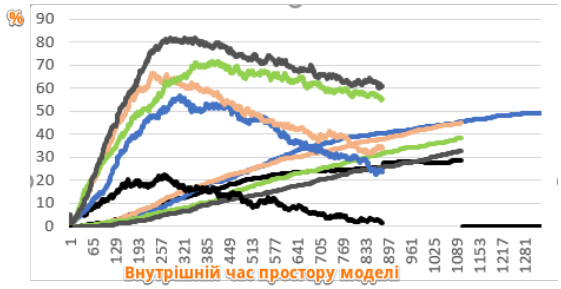

Рисунок 3 – залежність відновлення та зараження від параметру управління (virus-check-freq)

Рисунок 3 – демонструє динаміку адаптації системи з різними значеннями параметра virus-check-frequency (від 1 до 5), які відображені різними кольорами. Графіки показують, що зі збільшенням цього параметра від 1 до 5, система стає більш ефективною у виявленні вірусу та запобіганні його поширенню. Кожен сценарій позначено відповідним кольором .

На графіку видно, що при найнижчому значенні частоти перевірки (значення 1, синя лінія) вірус поширюється найбільш інтенсивно, тоді як при збільшеному показнику частоти перевірки до 5 (червона лінія), система значно швидше виявляє інфекції та дозволяє вузлам набувати стійкості до повторних заражень (збільшення кількості resistant вузлів). Це показує, що частіші перевірки значно знижують поширення вірусу, забезпечуючи стійкість системи до інцидентів у кіберпросторі.

Висновок. Мультиагентне моделювання у середовищі NetLogo є ефективним інструментом для імітації сценаріїв динаміки розвитку інцидентів, що надає можливість проводити аналіз ефективності заходів щодо протидії кіберзагрозам, розробляти стратегії швидкого реагування для відновлення систем, а також використовувати результати моделювання для візуалізації еволюції стану системи, в тому числі для організації навчання персоналу.

Література

1. NetLogo: Resources and Links URL:https://ccl.northwestern.edu/netlogo/resources.shtml;
2. Introduction to NetLogo URL:https://link.springer.com/chapter/10.1007/978-1-4020-5979-7_30.
3. Vestad, A., & Yang, B. (2024). A survey of agent-based modeling for cybersecurity. *Human Factors in Cybersecurity*.